DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

The present invention is a system and process for prescribing medications through the Internet using a medical prescription service website that is accessible to licensed users for entering and retrieving medical prescriptions. The term "Internet" encompasses the World Wide Web. Advantageously, the system and process is secured by encryption so that only users, the prescribing doctor and pharmacists for example, who are properly identified as an authorized user can enter the secured pages of the website. In this way, a doctor or his authorized medical personnel can enter a prescription quickly and easily onto the secured website of the medical prescription service. The pharmacy selected by the patient can access the medical prescription service website, locate the patient's record, obtain the prescription and fill it within minutes of entry by doctor. The prescription can be entered by any licensed medical doctor from anywhere in the world with access to the Internet, and filled by any pharmacy with access to the Internet. Patient information is secured though an encryption system thereby protecting patient privacy and medical information from the general public.

The users of the systems and processes of this invention are preferably limited to clients who are licensed physicians, their authorized personnel and licensed pharmacy personnel. Licensed physicians means licensed to practice medicine. Preferably, clients are authorized to use the system and processes of this invention by registration as illustrated in the flowchart of Fig. 7.

A licensed physician or pharmacist contacts the medical prescription service (mps) via its web home page, which is accessible to the general public. Alternatively the medical prescription service can be contacted by email, regular mail, fax, etc. Preferably, the potential client logs on to the website home page 710 and clicks onto a new user information form 715. The form is emailed to the medical prescription service 720. The medical prescription service verifies the professional license of the client 720 and assigns the client an encrypted login password or code 735. The encryption login code is securely transmitted to the client.

Clean Copy

Alternative methods of securing the medical prescription service website are sophisticated bodyscan coding. Bodyscan coding uses the client's eye, finger or hand prints to identify the client as an authorized user. The client's computer is adapted to scan the body part and transmit the information to the medical prescription service host computer which matches the scan to a list of authorized clients. Other methods of identifying the client so that only authorized users can access the sensitive information on the medical prescription service website can be also be used to limit access.

Payment for the service by the client physician or pharmacist can be made through a secure financial transaction system using a credit card. Secured financial transaction systems are known in the art available and easily available. Alternatively, direct banking or other methods of payment can be used.

Once the client has a secured, encrypted login password, the client can gain access to the medical prescription service website as illustrated in Fig. 1. Referring to the schematic of Fig. 1, the client doctor or pharmacy connects to the Internet by means of a general use computer 110, 115 via his or her own Internet Service Provider (ISP) 120, 125. The client can use any type of computer hardware that gives the client access to his or her ISP. New computer-type systems, not yet available, are within the scope of this invention if they enable access to the Internet and the website of the medical prescription service. The medical prescription service is contacted by way of its own ISP 130. The medical prescription service maintains a website having web pages for identification of clients, entry of prescriptions and patient, drug or medical informational databases. The introductory and login page(s) for the website are stored on the ISP 130 of the medical prescription service. Access to the introductory and login pages is available to the general public via the Internet.

Patient information, medical information databases, drug information databases and any other medically related database or sensitive data are stored on a remote server maintained by the medical prescription service. A server is a computer that is connected to one or more other computers allowing access to the data and programs stored on it.

Pending successful identification of the user as shown in Fig. 3, access to the remote server is only available to clients with a secured, encrypted pass code or I.D., body scan, for example. Absolutely no access to the remote server is permitted until after the visitor to the medical prescription service homepage correctly enters all of the necessary security information. This information would typically consist of a subscriber ID number, username and secured, encrypted password, code or bodyscan.

Upon verification of the login information, the medical prescription service ISP 130 accesses the remote server 135, which records a log of that client's admittance into the system, and presents the customer with a list of options, such as updating an existing patients' record, viewing a patient record, etc.

Patient records can be stored on a highly secure and recoverable storage system. Preferably, the backup system is a fail-safe system or safety check 250 that activates when the primary system fails so that there is no interruption of service. Other backup systems can also be used such as a RAID (Redundant Array of Inexpensive Disks), which is also backed up daily to an external medium 150 such as tape, removable disk or recordable CD. Should disaster strike and one or more of the drives in the array fail, the data can be restored via the other drives in the array or from the backup media. In case of catastrophe, such as fire, flood, or other non-recoverable destruction of patient records, a reasonably current copy of all data can be stored at a Remote/Off-site location 150.

A secure Internet information server is required for the medical prescription service of this invention. Preferably, the server can support a high bandwidth connection to the Internet, encryption and support for redundant and highly secure storage devices such as RAID (Redundant Array of Inexpensive Disks) controllers and removable media backups. Hardware and operating system software may vary. Encryption as use in reference to this invention is any procedure that converts data into a form that prevents anyone but the intended recipient from reading the encrypted data. Both Netscape's® Navigator™ and Microsoft's® Internet Explorer™ have encryption built in and automatically use it whenever transmitting data over a secure network. Preferably, other secure encryption programs can be used to

ensure that access to the medical prescription service website, other than the homepage, is limited to authorized clients. Alternatively, host Internet server systems are available that can provide a secured website. One such fully functional Internet server system is marketed under the trademark, VSERVER™.

High capacity storage and backup both on and off site are preferred. For primary storage, a ratio of less than one megabyte of storage per patient, physician and pharmacy can be used for storing patient prescription, physician and pharmacy identification information. Alternatively, the storage space can be increased or decreased depending on the amount of data regarding each patient that is desired. In one embodiment, about 10 to 20 gigabytes of additional storage are preferred for the system software and operating system. Again, the amount of storage space is dependent on the amount of data and databases the medical prescription service desires to be available to clients. Alternative embodiments of this invention can include a system and process of storing a patient's entire medical history as well as pharmaceutical information. These embodiments require additional storage space.

In one aspect of this invention, the Internet service provider can also store the encrypted patient information and drug prescription information. The preferred Internet service provider comprises a secure server that allows a remote server to be connected to its network. Storing the sensitive patient information and drug prescriptions on a remote server that is operated by the medical prescription service is an additional security precaution. Preferably, sensitive patient information is not stored by a third party server. Preferably, the data is not stored on a system shared by unauthorized users, vulnerable to hacking or other abuse. Control over backups and the integrity of patient information is paramount to the successful operation of this invention.

In an alternative system, security can be maintained through the use of "Digital Certificates, electronic files that act like an online passport. They are issued by a trusted third party, a certificate authority (CA), which verifies the identity of the certificate's holder. They are tamper-proof and cannot be forged. Both Netscape's® Navigator™ and Microsoft's® Internet Explorer™ (versions 3 and above respectively) support Digital Certificate. Access is available via

"http://home.netscape.com/security/techbriefs/index.html". An ODBC (Open Database Connectivity) compliant database in which to store patient records is also preferred. ODBC databases are accessible over a network and capable of being manipulated using Structured Query Language (SQL). SQL server software can be installed on the remote server to access and modify the patient database.

In one embodiment of the present invention, the user/client accesses the website via the Internet. The homepage for the website can reside on the medical prescription service's ISP (Internet Service Provider) and consists of an introductory splash screen along with links to information about the site and its services, contact information, and membership application, as well as a link for accessing patient information. At this level, all website information resides on the ISP. Absolutely no access to the remote server containing crucial and sensitive patient information or databases is permitted until after the visitor passes all necessary security.

Preferably, the user enters an ID, body scan, username or password before gaining access to the remote server. Upon verification, the ISP connects to a remote server using an encrypted and secure link. "Encryption" refers to the encoding of information transmitted over the Internet to prevent it from being read by anyone without the proper authorization. Encryption is built in to the most popular web browsers in use today (Microsoft's® Internet Explorer™ and Netscape's® Navigator™/Communicator Suite™) and is performed automatically. "Encryption challenged" web browsers will not be permitted to enter the system.

The remote server then acknowledges or identifies the client by name and presents the client with a menu of available options. The client enters the identifying information of the patient whose records they wish to access. This can comprise the patient's name, ID number, social security number, driver's license number, phone number, or any combination thereof. The system then retrieves the patient's record and displays any pertinent information and/or a menu of options. Alternatively, the doctor/client can create a patient record file with patient identifying information as illustrated in Fig. 4.

Patient records are then accessed and displayed for the client. If changes or updates are made to the patients record, such as the addition of a new prescription,

the system then can check the new medication against the list of other drugs and therapies the patient may be under. This check searches for dangerous drug interactions or any activities that should not be followed while using said medication. Only doctors with the proper authorization code are allowed to make changes to a patient record.

After the doctor or one his authorized medical personnel enters the prescription, the doctor can request another patient record or log off. If the doctor/client fails to log off, automatic log off occurs within a specific period of time, fifteen minutes for example.

The patient, patient's representative or doctor can then contact a client pharmacy to have the prescription filled.

The client/pharmacy, registered according to the flowchart of Fig. 7, connects to the Internet by means of a computer and its ISP. As depicted in Fig. 6, it accesses the medical prescription service's home web page, enters its I.D., pass code or body scan and is connected to the patient record. The pharmacy can download the prescription or make a hard copy so that prescription can be filled. The client/pharmacy then records that prescription is filled and logs off. Automatic log off occurs within a specific period of time, fifteen minutes for example. The pharmacy can make a further request. The system then reports back to the client the results of their request regarding databases or links available on the medical prescription service website. From there, the pharmacy/client can either modify their request, access another patient record or logoff.

The foregoing description is illustrative and explanatory of preferred embodiments of the invention, and variations in the size, shape, materials and other details will become apparent to those skilled in the art. It is intended that all such variations and modifications which fall within the scope or spirit of the appended claims be embraced thereby. Although described in terms of the preferred embodiments shown in the figures, those skilled in the art who have the benefit of this disclosure will recognize that changes can be made to the individual steps which do not change the manner in which the system and process achieve their intended

result. All such changes are intended to fall within the scope of the following non-limiting claims.